

Complying with FACTA “Red Flag” Rules



By Ann Bachman, MT (ASCP), CLC (AMT)

The Federal Trade Commission (FTC), the National Credit Union Administration (NCUA), and various banking agencies issued the Fair and Accurate Credit Transactions Act (FACTA, aka Red Flag Rules), requiring financial institutions and creditors to establish and enforce written identity protection programs. The original compliance date was November 1, 2008, but was extended first to May 1, 2009, and then to August, and finally to November 1, 2009. The main reason for delaying enforcement was that many of the institutions subject to these regulations (including physician practices) were either unaware of the rules or unaware they were subject to the regulations.

The purpose of these rules is to protect financial information associated with patients, employees and employers, thereby preventing identity theft, similar to the way HIPAA is aimed at preventing inappropriate release of private health information. For medical practices, the primary Red Flag concern is medical identity theft, which occurs when one individual uses information about another patient to obtain care fraudulently.

The American Medical Association has challenged the interpretation that the Red Flag Rules cover physician practices. While doctors' offices are not officially financial institutions, they may indeed meet the official FTC definition of “creditor.” Two factors contribute to the FTC's determination:

- Physician practices typically allow patients to make payments over time rather than require full payment in one transaction.
- Practices usually bill the insurance company first and then bill the patient for the remainder.

A “creditor,” according to FACTA, is “any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit. . .”

According to at least one interpretation, accepting one-time credit card payments does not in itself make an entity subject to the FACTA rules. Allowing multiple payments for one service or product does make the entity a “creditor” and, therefore, subject to the rules.

Entities subject to the regulation must have a written program that:

1. Is developed or managed by the board of directors or senior employees,
2. Includes information on how to recognize potential financial problems (“red flags”),
3. Tells the staff how to respond to these red flags,
4. Is designed to fit the size and complexity of the entity,
5. Allows flexibility to revise the plan when new risks are discovered, and
6. Provides for staff training.

Some examples of “red flags”:

- Two or more patients give the same Social Security number.
- A patient calls with concerns about a bill or an Explanation of Benefits for a service that the patient denies receiving.
- Necessary documentation such as the patient's insurance card is not provided.
- Documentation provided appears to be altered or fictitious.
- The practice receives a fraud alert from an insurance company or another agency.
- The patient does not resemble a picture on file.
- The patient's signature does not match the signature on file.

When an employee notices something that may be a red flag, he or she should gather all documentation available, document the incident, and report the incident to the designated individual. This individual, who may be a supervisor or the privacy officer, should review the information to determine if further action is needed. This person may determine that the incident does not

require further action, in which case the situation will be noted. However, if suspicion remains, the person in charge may decide to implement one or more of the following actions:

1. Review the incident with the physician to see if there are inconsistencies in the medical record.
2. Cancel the financial transaction.
3. Notify the patient of the incident.
4. Notify the police or other pertinent agency.

If the patient claims to be a victim of identity theft, the patient should be directed to contact the police, to complete the FTC's *ID Theft Affidavit*, and to report the incident to one of the three national credit card bureaus. The physician should review the medical record to ensure that no erroneous information is present and should create an addendum to correct any inconsistencies.

The FACTA rules do require employee training, but no specifications about the type of training are included. Therefore, we have concluded that reviewing the policy with the employees and having them sign an acknowledgement statement should suffice.

Many agencies, including the American Medical Association (www.ama-assoc.com) and DoctorsManagement (www.drsmgmt.com), have sample plans available on their respective web sites at no cost. However, the cost for failure to comply by the deadline is a penalty of \$2,500. +

Ms. Bachman is director of the Compliance Department at DoctorsManagement. You can contact her at abachman@drsmgmt.com or 800-635-4040.

DoctorsManagement, LLC, is a TMA Corporate Partner. *This information was supplied by DoctorsManagement exclusively and for the benefit of our members. The TMA does not accept responsibility for the information provided.*